Remarks

Applicants respectfully request reconsideration of this application as amended. Claims 1-3, 8, 10 and 13 have been amended. No claims have been cancelled. Therefore, claims 1-15 are presented for examination.

Claim 13 stands rejected under 35 U.S.C. §112, second paragraph. Applicant submits that claim 13 has been amended to appear in proper condition for allowance.

Claims 1, 2, 10, 13 and 14 stand rejected under 35 U.S.C. §102(e) as being anticipated by Cromer et al. (U.S. Patent No. 6,684,326). Further, claim 7 stands rejected under 35 U.S.C. §103(a) as being unpatentable over Cromer with Official Notice taken. Applicant submits that the present claims are patentable over Cromer.

Cromer discloses a method and system for performing an authenticated boot of a computer system in a networked computing environment are provided. The method and system include integration of boot manager services into a power on self test (POST) routine of a client system. The client system provides a digital signature for a selected operating system when the POST routine transfers control to a basic input/output system (BIOS) routine. Booting is authorized with the operating system through authentication by a server system of the digital signature. See Cromer at Abstract.

Claim 1 of the present application recites an authentication stack having a control layer to control authentication, an interface layer to define function calls, a support layer to translate the function calls received from the interface layer into proprietary calls and a hardware layer having one or more hardware devices. Applicant submits that nowhere in Cromer is there disclosed or suggested an authentication stack having the described layers. Therefore claim 1 and dependent claims 2-15 are patentable over Cromer.

Claims 3, 4, 8 and 9 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Cromer, in view of Angelo et al. (U.S. Patent No. 5,953,422). Applicant submits that the present claims are patentable over Cromer even in view of Angelo.

Angelo discloses a computer system incorporating a two-piece authentication procedure for securely providing user authentication over a network. a user password is entered during a secure power-up procedure. The user password is encrypted by an external token or smart card that stores an encryption algorithm furnished with an encryption key that is unique or of limited production. A network password is thereby created. The network password is maintained in a secure memory space such as System Management Mode (SMM) memory. The network password is then encrypted and communicated over the network. The network password may be encrypted using the server's public key or another key that is known to the server. Optional node identification information is appended to the network password prior to communication over the network. Once received by the server, the encrypted network password is decrypted using the server's private key. A user verification process is then performed on the network password to determine which, if any, access privileges have been accorded the network user. See Angelo at Abstract.

However, Angelo does not disclose or suggest an authentication stack having a control layer to control authentication, an interface layer to define function calls, a support layer to translate the function calls received from the interface layer into proprietary calls and a hardware layer having one or more hardware devices. As discussed above, Cromer also fails to disclose or suggest an authentication stack having a control layer to control authentication, an interface layer to define function calls, a support layer to translate the

function calls received from the interface layer into proprietary calls and a hardware layer having one or more hardware devices. Thus, any combination of Cromer and Angelo would not disclose or suggest an authentication stack having a control layer to control authentication, an interface layer to define function calls, a support layer to translate the function calls received from the interface layer into proprietary calls and a hardware layer having one or more hardware devices. As a result, the present claims are patentable over Cromer in view of Angelo.

Claims 5, 6, 11 and 12 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Cromer, in view of Angelo, further in view of Novoa et al. (U.S. Patent No. 6,223,284). Applicant submits that the present claims are patentable over Cromer and Angelo even in view of Novoa.

Novoa discloses a remote flash ROM and security package formed and delivered to a system ROM of a target computer system for remote flashing of the ROM and remote configuration of security settings for the computer system. See Novoa at Abstract. Nevertheless, Novoa does not disclose or suggest an authentication stack having a control layer to control authentication, an interface layer to define function calls, a support layer to translate the function calls received from the interface layer into proprietary calls and a hardware layer having one or more hardware devices.

As discussed above, neither Cromer nor Angelo disclose or suggest an authentication stack having a control layer to control authentication, an interface layer to define function calls, a support layer to translate the function calls received from the interface layer into proprietary calls and a hardware layer having one or more hardware devices. Thus, any

combination of Cromer and Angelo would not disclose or suggest such a feature. As a result, the present claims are patentable over the combination of Cromer, Angelo and Novoa.

Claim 15 stands rejected under 35 U.S.C. §103(a) as being unpatentable over Cromer, in view of Angelo, further in view of Bisbee (U.S. Pub. No. 2001/0002485). Applicant submits that the present claims are patentable over Cromer and Angelo even in view of Bisbee.

Bisbee discloses a method of handling stored e-original objects that have been created by signing information objects by respective Transfer Agents, submitting signed information objects to a TCU, validating the submitted signed information objects by at least testing the integrity of the contents of each signed information object and the validity of the signature of the respective Transfer Agent, and applying to each validated information object a date-time stamp and a digital signature and authentication certificate of the TCU. See Bisbee at Abstract.

Nonetheless, Bisbee does not disclose or suggest an authentication stack having a control layer to control authentication, an interface layer to define function calls, a support layer to translate the function calls received from the interface layer into proprietary calls and a hardware layer having one or more hardware devices. As discussed above, both Cromer and Angelo fail disclose or suggest such a feature. Thus, any combination of Cromer and Angelo would not disclose or suggest the feature. As a result, the present claims are patentable over the combination of Cromer, Angelo and Bisbee.

Applicants respectfully submit that the rejections have been overcome and that the claims are in condition for allowance. Accordingly, applicants respectfully request the rejections be withdrawn and the claims be allowed.

The Examiner is requested to call the undersigned at (303) 740-1980 if there remains any issue with allowance of the case.

Please charge any shortage to our Deposit Account No. 02-2666.

Respectfully submitted,

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP

Date: July 15, 2005

Mark L. Watson
Reg. No. 46,322

12400 Wilshire Boulevard
7th Floor
Los Angeles, California 90025-1026
(303) 740-1980